Microsoft Exchange Server

Chapter 3
Configuring the Active Directory Connector

Deployment Guide

Abstract

This chapter describes the purpose and features of the Exchange 2000 Active Directory Connector (ADC), and illustrates how to properly configure it to achieve coexistence with your existing Exchange 5.5 environment. Topics include how to use the ADC in single and multi-organization scenarios, as well as the step-by-step process for configuring the ADC in these situations.

If you are not upgrading from Exchange 5.5 or will not be deploying multiple Active Directory forests you can skip this chapter.

This is a preview edition of the Microsoft Exchange 2000 Server Upgrade Series. The final documentation will be available in November 2000.

© 2000 Microsoft Corporation. All rights reserved.

THIS IS PRELIMINARY DOCUMENTATION. The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Microsoft, Active Directory, Windows, Windows NT and the Windows logo are registered trademarks of Microsoft Corporation.

Other product or company names mentioned herein may be the trademarks of their respective owners.

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

1000

CONTENTS

INTRODUCTION.....1
Exchange 5.5 and Exchange 2000 Coexistence Design Considerations 1
The Active Directory Connector 1
MMS Inter-Forest Toolkit 3
Active Directory Connector Configuration and Operational Requirements 4
Before Configuring the ADC or Installing MMS 5
Active Directory Connector 5

INTRAORG – A SINGLE EXCHANGE ORGANIZATION.....6
What you will need (Resources) 6
What you should know (Data) 6
Step-By-Step Procedure 6
Fallback Plan 7
Related Topics 8
Versions of the ADC 8
Windows 2000 ADC 8
Exchange 2000 Server ADC Update 8

INTERORG – MORE THAN ONE EXCHANGE ORGANIZATION.....9
What you will need (Resources) 9
What you should know (Data) 9
Step-by-Step Procedure 9
Fallback Plan 10
Related Topics 10

SUMMARY.....11
More Information 11

INTRODUCTION

The full integration of Exchange 2000 with Windows 2000 Active Directory can pose a number of challenges when you want to link to an existing Exchange 5.5 environment. Depending on your Exchange 5.5 architecture, you might have a large number of sites and organizations, a small number of sites and organizations, or some combination in the middle of that spectrum. To provide coexistence for Exchange 2000 with your existing environment, you will need to install and configure the Active Directory Connector (ADC), which replicates mailbox, distribution lists, and routing information between Active Directory and the Exchange 5.5 directory.

Some companies (for example, LIC) implement multiple Exchange organizations, using multiple Exchange 5.5 organizations or separate Windows 2000 Active Directory forests, within their environment. Implementing multiple organizations introduces a number of challenges, including synchronizing user, group and distribution list information between these organizations.

Note that the ADC is designed to provide coexistence for an eventual migration to Exchange 2000. It is not designed to be a long-term solution for coexistence.

The coexistence options discussed in this chapter are:

- **Intra-org:** the Exchange 5.5 and Exchange 2000 systems are configured with the same organization name.
- **Inter-org:** one or more Exchange 5.5 organizations are using a different organization name than the Exchange 2000 system.

Exchange 5.5 and Exchange 2000 Coexistence Design Considerations

Coexistence of Exchange 2000 can be broken into three categories:

- Coexistence between Exchange 5.5 and Exchange 2000
- Coexistence between two or more Exchange 2000 forests
- Coexistence with another messaging system like Lotus Notes or cc:Mail

This section will discuss the solutions and design considerations concerning coexistence options one and two; number three is covered separately in the migration whitepapers available at http://www.microsoft.com/exchange.

The Active Directory Connector

You have probably spent a considerable amount of time and effort in designing and deploying your Exchange 5.5 environment, so you want to make sure your Exchange 2000 environment makes use of that work. The

Preview Documentation

ADC included with Exchange 2000 is required to migrate from Exchange 5.5 to Exchange 2000. The ADC synchronizes two distinct types of objects:

- **Recipients** (Mailboxes, Distribution Lists, Custom Recipients)
- **Configuration information** (Connectors, Monitors, Protocols)

The ADC replicates those objects by:

- Using the LDAP Application Programming Interfaces (APIs) to perform fast replication between the Exchange 5.5 directory service and Active Directory.
- Hosting all active replication components on Active Directory, not on Exchange 5.5.
- Whenever possible, replicating only the changes between the directories.
- Maintaining object fidelity through replication (for example, the Active Directory Group object maps to the Exchange Distribution List object).
- Hosting multiple connections on a single server and managing these through Connection Agreements (CAs).

Important considerations looking at how to achieve coexistence between Exchange 5.5 and Exchange 2000 include:

- The number of Exchange 5.5 organizations
- The number of Exchange 5.5 sites
- The types of objects that need to be replicated (users, distribution lists, public folders)

The Exchange 5.5 recipient objects become one of the following native Windows 2000 objects in the Active Directory domain container:

- **Mailbox**: an Exchange 5.5 mailbox becomes a Windows 2000 user who has been mailbox-enabled: in other words, a user with an email address. The email address describes the Exchange server to which the user's mail should be routed, and to which the user connects to receive mail. Mailbox-enabled users are security principals (with logon rights) in Active Directory that can send and receive messages. Implicitly, these user types also have Simple Mail Transfer Protocol (SMTP) addresses.
- **Distribution Lists**: Windows 2000 uses groups to reduce the number of objects that require direct administration. Users are placed into groups, which are further consolidated into other groups, allowing bulk administration. Exchange 2000 Server uses this concept of bulk administration and permission granting, but it also uses groups as distribution lists to which you can send messages. Active Directory supports two types of groups, Security and Distribution, each of which can be mail-enabled, and scoped to Domain Local, Global, and Universal groups within Windows 2000.
- **Custom Recipients**: In general, an Exchange 5.5 Custom Recipient is represented as a mail-enabled Contact in Active Directory; that is, a Contact with an email address and (optionally) information that

allows Exchange to properly route the mail. All mail-enabled contacts can have either an SMTP address, or a target address that points to the system on which they reside: like Lotus Notes or an X.400-based system.

The CA is like the work order to the replication engine: defining replication characteristics such as the server names to contact for synchronization, object classes to synchronize, target containers, and synchronization schedule. A single ADC can host multiple CAs—each connecting Active Directory to a single Exchange Server site, or to multiple Exchange Server sites (one per CA).
Specifically, a connection agreement defines the following:

- Directory(s) to be synchronized.
- Windows 2000 Server synchronization objects.
- Exchange Server 5.5 synchronization objects.
- The direction in which synchronization takes place, either one-way or two-way.
- Synchronization schedule, which directly affects server processing load.

It is important to note that computers running the ADC are appropriately specified (CPU and memory) and well-connected (LAN speed). The default synchronization schedule is 8 hours, but may be adjusted for each CA in the case of multiple CAs to one Exchange 5.5 site for more granular container control. For example, you can set one CA schedule to once per week, and another to once per day.

- Method for deleting objects.
- Advanced options, including:
  - Attribute mapping.
  - New object creation.
  - Authenticating Directories.
  - Specifying which OUs or containers to synchronize.

Since each connection agreement maps a single recipient's container root in Exchange to an organizational unit or container in Active Directory, you need at least one CA for every recipients container you use. Additionally, if you will be writing changes back to the Exchange 5.5 objects from updates in the Active Directory you will need one CA per Exchange 5.5 site, since objects can only be updated in an the Exchange 5.5 site in they reside.

MMS Inter-Forest Toolkit

In July of 1999, Microsoft acquired the company named Zoomit to develop their Metadirectory product called VIA. This product was re-branded Microsoft Metadirectory Services (MMS), and was re-released in July 2000 in Version 2.2. MMS specifically solves the identity problem for large companies with many disparate directories containing valuable user attribute information. MMS provides attribute brokering and account provisioning services to the Windows 2000 platform.

Active Directory Connector Configuration and Operational Requirements

This section discusses the ADC installation and configuration requirements.

Installation requirements

The ADC must be installed on a Windows 2000 server that is a domain controller in the domain for which the ADC will manage objects. It will run on Windows 2000 Server or Windows 2000 Advanced Server.

Note: If you are looking at deploying Windows 2000 DataCenter Server, adding software such as the ADC should be the responsibility of your solution provider.

Before deploying the Active Directory Connector (ADC) and creating CA, it is crucial that all pertinent business requirements are taken into account in order to avoid problems later on. You can configure the ADC to make fundamental changes to directories (including deleting objects). Therefore, incorrect deployment can result in destabilization of your existing Exchange infrastructure.

Installation Time Factors

It should take less than an hour to install the ADC in most environments, but it can take anywhere from a few hours to a few days for you to create the CAs. The time required depends upon the number of CAs involved and the complexity of your recipient container mapping to Active Directory.

For a 5,000 user system, plan for at least two hours to install a one-way CA and have it replicate all the changes to Active Directory or Exchange 5.5. For two-way agreements, allocate at least five hours for the changes to be replicated to both directories. The length of time for your particular implementation depends upon the number and type of objects in the directory that you are replicating. Essentially, plan for the initial replication cycle to be a time consuming process, but any subsequent incremental updates should be relatively quick. Keep the time it takes to do the first full replication in mind in case you decide to force a full replication, as you can use that to estimate how long a full update will take.

Operational requirements

As a general rule, ADC operation requires no more time or effort than any other service included with Windows 2000. All errors and warnings are written to the Windows 2000 Event Log, so monitoring this allows you to determine the health of the ADC and alerts your support staff to any issues.

INTRAORG – A SINGLE EXCHANGE ORGANIZATION

Any unplanned operations, like a forced full update, will require you to keep a closer eye on the CA processes running under the ADC. This process should normally be done during the maintenance window dictated by your organization's SLA, so that the least impact on Active Directory replication and user access is felt.

Before Configuring the ADC or Installing MMS

The next section covers the steps and actions that you should complete before you configure the ADC CAs.

Active Directory Connector

Installation of the ADC will affect Active Directory, the Schema, and the Exchange 5.5 Directory.

Windows 2000 Active Directory Requirements and Impact

The ADC requires:

- Schema extensions to the Active Directory, which require the Schema Admins permission
- The use of a service account that has Domain Administrator permissions in the domain.

Schema Requirements and Impact

The schema must be extended to support the functionality of the ADC. This is done at the time that the ADC is installed. Since a number of these attributes are promoted to the GC, the effect of installing the schema extensions within the ADC is a full replication of the Active Directory forest. You should plan on installing the ADC during non-business hours to minimize this impact, and monitor the replication to make sure it completes correctly.

Exchange 5.5 Requirements and Impact

The ADC requires Exchange 5.5 Service Pack 3 to be installed on the server that the ADC will access. When you install Service Pack 3, the Exchange 5.5 schema is extended to support the ADC and will also cause a full synchronization of the Exchange 5.5 environment. Experience has proven that the installation of Service Pack 3 in a production environment has minimal impact if proper planning and risk mitigation are performed. For more information on installing Exchange 5.5 Service Pack 3, see http://www.microsoft.com/exchange/downloads/sp3.htm.

The Intra-Organization replication is the simplest to configure and is the most common arrangement for directory synchronization.

Preview Documentation

What you will need (Resources)

To create an Intra-organizational connection agreement you will require:

- Windows 2000 Server or Advanced Server.
- Active Directory Connector installed on a Windows 2000 Domain Controller.
- Exchange 5.5 Service Pack 3.

What you should know (Data)

In addition, you will need to know the following:

- Name of the Exchange 5.5 organization to which you are connecting.
- Name of the service account for the Active Directory ADC CA.
- Name of the service account used to access Exchange 5.5.
- Name of the Exchange server and site to which you are connecting.
- IP address of the target server
- Name of an OU or container in the AD in which you will create user accounts from the Exchange 5.5 organization. This could be the default Users container, or it could be a separate OU that you create using the Active Directory Users and Computers console.

Since the intra-org CA is designed to be a migration tool to move from an Exchange 5.5 environment to an Exchange 2000 environment, it is important for you to have already determined which objects from the Exchange 5.5 sites will be represented in Active Directory.

Step-By-Step Procedure

To carry out this procedure, perform the following steps:

1. Login to Windows 2000 with an domain administrator account.
2. Open the **Active Directory Connector** MMC console
3. Expand the **Active Directory Connector Management** container, then right- click on the **Active Directory Connector** object.
4. Point at **New**, then click **Recipient Connection Agreement**
5. For the **Name:** field, enter *Connection to XXXX* where *XXXX* is a name that is clear and intuitive.
6. Configure the direction as either one-way (From Exchange to Windows) or two-way, depending on the criteria evaluated earlier in this chapter.
7. Click the **Connections** tab and, in the **Windows Server Information** textbox, click **Modify** for the **Connect as** option. Click **Browse** and select the service account that you will use for the ADC, then click **OK**. Enter the appropriate password for this service account and click **OK**.

8. For the **Exchange Server Information**, enter the name of the Exchange server to which you will be connecting.

NOTE: You must enter the Exchange server name and IP address in the LMHOSTS file if you cannot resolve the machine using DNS or WINS.

9. Click **Modify** next to the **Connect as** textbox. In the **Connect as** textbox, enter the string *DOMAIN\Account*" where *Domain* is the Windows NT domain and *Account* has the appropriate permissions to the Exchange server you are accessing. Enter the appropriate password and click **OK**.
10. Click the **Schedule** tab, and set the schedule to **Always** (that is, every 15 minutes). Optionally, you can configure the connection to run at specific times of the day.
11. Click the **Advanced** tab, and change the **Paged results** values to **99** for both the **Windows Server entries per page** and the **Exchange Server entries per page**.
12. Click the **From Exchange** tab and then click the **Add** button underneath **Choose the Exchange recipients containers to take updates from** to select the containers to import. Select the containers you want to import and click **OK**. Repeat as necessary, choosing other sites and containers if the Exchange system has multiple sites or containers.
13. Click **Modify** next to the **Default destination** textbox. Select the OU container in which you want the ADC to create new accounts. (This is the OU that you identified in the *What you should know* section.) Click **OK**.
14. Choose which objects to replicate by checking or un-checking the selections shown in the scrolling listbox. Deselect the mailboxes and distribution lists selection unless you need to replicate custom recipients as well as mailboxes and distribution lists.
15. Click **OK** to save changes, then right-click the new connection and click **Replicate now** to force the first replication. Verify that the objects are showing up in the OU container in Windows 2000 and the ADC is not generating any errors in the Application Event Log.

Fallback Plan

Removing a CA and removing its effects are very delicate processes. If you are not careful, you might delete objects in Active Directory or Exchange 5.5, which would require a complete system restore to recover. If you decide to remove a CA you just configured, the first thing you should do is configure that CA to save deletes to a file instead of writing them to the directory service. This way, if something goes wrong, all you

INTERORG – MORE THAN ONE EXCHANGE ORGANIZATION

will end up with is a file of deletes: not actual deletes. For more information on this topic see the TechNet articles Q254821 and Q249831.

Once you have properly removed the CA, you can clean up the accounts it created. This is best accomplished using the Active Directory Users and Computers MMC, or using an ADSI script. Depending on your requirements, you may not need to delete the objects the ADC created, and in this case you are finished rolling-back.

Related Topics

For information on installing the ADC, see the “Install Active Directory Connector” section of Chapter 2 in this deployment guide.

Versions of the ADC

There are two version of the ADC available, and their differences are described below. One of these you should use, the other you shouldn’t. See if you can spot which is which.

Windows 2000 ADC

This version shipped with Windows 2000, and replicates rich directory information in Exchange 5.5 to Active Directory and vice versa. Many customers have already invested heavily in the Exchange 5.5 directory, and much of this data can be bulk uploaded to Active Directory, thus decreasing implementation time. Through synchronization, the Active Directory administrator can also achieve basic management of the Exchange 5.5 users.

Exchange 2000 Server ADC Update

This is an enhanced connector that ships with Exchange 2000 Server. Whereas the Windows 2000 ADC simply replicates objects in the Exchange site naming context (for example, **Recipients** containers) to the Active Directory, the Exchange 2000 ADC also replicates data from the configuration naming context, thus providing support for mixed-mode Exchange sites and downstream routing.

So you guessed, it’s the second one that you need for integration between Exchange 5.5 and Exchange 2000.

Inter-organizational replication is a slightly more complex scenario, requiring you to select an extra checkbox.

What you will need (Resources)

To carry out this procedure, you will require the following resources:

- Windows 2000 Server or Advanced Server
- Active Directory Connector installed on a Windows 2000 Domain Controller
- Exchange 5.5 service pack 3

What you should know (Data)

You need to know the following information:

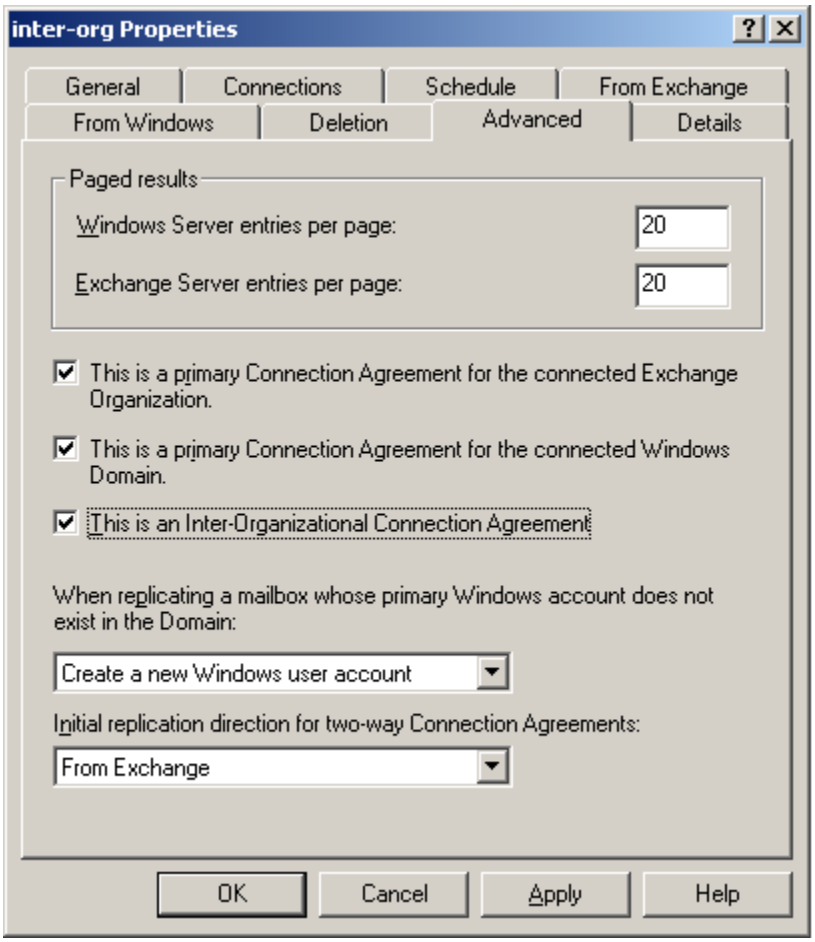
- Name of the Exchange 5.5 organization to which you are connecting
- Name of the service account for the Active Directory ADC CA
- Name of the service account used to access Exchange 5.5
- Name of the Exchange server and site you will connect to
- IP address of the server you will connect to
- Name of the OU or container in the AD in which you will create contacts for the users from the Exchange 5.5 organization

Step-by-Step Procedure

Configuring an ADC in an inter-organizational scenario requires the same steps as for an intra-organization replication, with the addition of these steps:

- On the step when you change the paged results values to 99 for both the Windows and Exchange servers, you must also check the box that indicates **This is an Inter-Organizational Connection Agreement**.
- Next, you will click the **From Exchange** tab and click **Add** to select the containers to import. Make sure the **SITE,ORG** are highlighted and click **OK**. Repeat choosing other sites and containers if the Exchange system has multiple sites or containers.
- When you are offered a list from which to choose which objects to replicate, check the only mailboxes selection unless advised otherwise.

For an inter-org CA to work, you must check the **This is an inter-Organizational Connection Agreement** statement in the **Advanced** page of the CA, as shown here. This will create contact items in Active directory to represent the users from the Exchange 5.5 organization.



Fallback Plan

Since you are creating an inter-organizational CA, the only objects it will create are contacts in the AD and Custom recipients in the Exchange 5.5 directory. Since contacts and custom recipients do not have any security credentials in the directory in which they exist, it is fairly easy to delete these entries without any major repercussions. Mostly, you need to be aware of groups and their memberships when you clean up an inter-org CA, since you probably do not want to re-create those groups in the future. Simply delete the contacts in the AD and the Custom recipients in the Exchange 5.5 container you put them in, and as long as the CA is not running, everything should be cleaned up.

Related Topics

“Exchange Server 5.5 Interorganizational Solutions”
http://www.exchangeadmin.com July 2000 issue

Exchange 2000 resource kit chapter 20 (ISBN 0-7356-1017-7)

TechNet article Q264482 “Support Boundaries for ADC Inter-Org Synchronization”

SUMMARY

This chapter covered the synchronization of Exchange 5.5 and the Active Directory. The processes and solutions outlined in this chapter involved in setting up Inter-Organizational solutions may look complex but are in fact, fairly straightforward tasks to carry out. If you have one or more Exchange 5.5 organizations that you need to synchronize with Active Directory for the purposes of migration, then the Active Directory Connector included with Exchange 2000 is the best solution.

More Information

For more information on the ADC, see the following links:

Guide to upgrading from Exchange Server 5.5 to Exchange 2000 Server

Exchange 2000 Deployment Guide: Chapter 20 – Synchronizing Active Directory with Exchange Server Directory Service

http://www.microsoft.com/windows2000/mms

http://www.microsoft.com/windows2000/guide/server/features/directory.asp